AMENDMENTS TO THE SPECIFICATION:

Page 1, amend the paragraph beginning at line 16 and continuing to page 2, line 7 as follows:

Whilst it is desirable to provide mechanisms that can enforce the banning of certain computer programs, it is advantageous if these mechanisms do not themselves represent a significant additional overhead in terms of installation, maintenance and consumption of processing resources. To this end, it has been proposed that banned computer programs could be treated as if they were computer viruses and the mechanisms that are already in place upon many computer systems to combat computer viruses be used to enforce the banning undesired, although not actually virus-like, computer programs. Whilst such an approach is superficially attractive as it could effectively prevent execution of unwanted computer programs without requiring an addition system and without consuming significant additional processing resources, it has the disadvantage that there is no universally accepted view of which computer programs should be banned from use. In some ~~organisations~~organizations, it may be entirely acceptable for games to be executed on computer systems, whilst in other ~~organisations~~organizations this may be strictly prohibited. Accordingly, the anti-virus computer system provider would need to produce a wide set of banned computer program definition data such that individual users could pick the appropriate definition data to ban their particular set of unwanted computer programs. This would represent an impractical additional overhead on the anti computer virus system provider as a very large number of different banned program definition files would be required. Furthermore, it is undesirable for the anti-computer virus program provider to become involved in deciding which computer programs are potentially of a sort that a user may wish to ban.

Page 2, amend the paragraph beginning at line 20 as follows:

The invention preserves the desirable characteristics of ~~utilising~~utilizing the anti-computer virus systems to enforce computer program banning whilst avoiding the disadvantages of requiring the system provider to produce many different banned computer program identifying data types by providing a tool to end users to themselves specify their own collection of computer programs that they wish to ban from their systems. This tool can then be used to generate banned program identifying data that interfaces with and controls an anti computer virus system to take banning measures against those computer programs specified as banned by a particular user.

Page 2, amend the paragraph beginning at line 28 and continuing to page 3, line 10 as follows:

It will be appreciated that the generation of anti-computer virus definition data relating to banned programs by end users could lead to misuse with malicious persons introducing definition data that treated some essential or desired computer program as banned when this was not intended. In order to help resist this, preferred embodiments of the invention are such that the tool only produces encrypted banned program identifying data using a private key. This encrypted data will only be decrypted into a form where it is usable by computer programs having a corresponding matching public key. Thus, banned computer program identifying data can be made specific to a particular ~~organisation~~organization such that will not be effective if it propagates outside of that ~~organisation~~organization. Furthermore, unless a set of banned computer program identifying data was produced using the private key corresponding to a

particular machine's public key, then that definition data will not operate on the computer with the public key.

Page 3, amend the paragraph beginning at line 17 as follows:

In a highly secure environment, the system may be ~~utilised~~utilized to produce banned computer program identifying data that effectively comprises a list of permitted computer programs with all computer not matching that list being treated as banned.

Page 5, amend the paragraph beginning at line 10 as follows:

Figure 1 illustrates an operating system 2 that co-operates with an anti-virus system 4. In use, file access requests are received by the operating system 2 as a result, for example, of application program use or user commands. A file access request is intercepted before it is serviced by the operating system and information ~~characterising~~characterizing the file access request is passed to the anti-virus software 4. This information can include details such as the file name, the access requester, the location of the computer file requested, etc. The anti-virus software 4 uses this information to trigger an anti-virus engine 6 in conjunction with virus definition data 8 to perform an anti-virus scan of the computer file concerned. Such scans may be performed upon an on-access basis as described above or on an on-demand basis as part of regular thorough scan of an entire system. If the computer file in question passes the anti-virus scan, then a pass signal is returned to the operating system 2 which can then continue to service the file access request using, for example, a hard disk drive 10 storing the computer file.

Page 6, amend the paragraph beginning at line 19 as follows:

Once the user has assembled the collection of computer files that they wish to be treated as banned, step 16 is performed to generate a set of banned computer program identifying data that may be ~~utilised~~utilized by the anti-virus software 4.

Page 6, amend the paragraph beginning at line 26 as follows:

The banned computer program identifying data can look for key executable computer instruction sequences within the computer files concerned or alternatively/additionally identify heuristic ~~behavioural~~behavioral characteristics of that computer program that may be ~~analysed~~analyzed in a manner that provides a degree of protection against variants of that computer program.

Page 7, amend the paragraph beginning at line 10 as follows:

In order to provide resistance against the system being used maliciously, the banned computer program identifying data is encrypted using the private PGP key of the ~~organisation~~organization generating it at step 18. Encrypting the data in this way has the result that only a computer using the corresponding public key will successfully decrypt it so rendering the widespread distribution of malicious banned computer program identifying data file less likely.